

Configurar o buraco negro disparado remoto IPV6 com BGP IPV6

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração relevante](#)

[Verificar](#)

[Caso de teste 1](#)

[Teste do caso 2](#)

[Caso de teste 3](#)

[Troubleshoot](#)

Introduction

Este documento descreve o comportamento visto com IPV6 Remote Triggered Black Hole (RTBH). Ele mostra um cenário em que o tráfego IPV6 é intencionalmente suspenso em preto usando um mapa de rotas.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IPV6
- BGP (Border Gateway Protocol)

Componentes Utilizados

As informações neste documento são baseadas na versão 15.4 do software Cisco IOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

A filtragem RTBH é uma técnica geralmente empregada para evitar ataques de negação de serviço (DoS). Um problema comum observado com ataques de DoS é que a rede é inundada com grandes volumes de tráfego indesejado/mal-intencionado. Isso resulta em estrangulamento de links e outros problemas, como alta CPU etc. Isso elimina o tráfego legítimo e resulta em implicações sérias na rede.

Conforme RFC 2545, o endereço de link local será incluído no campo Next Hop se e somente se o locutor BGP compartilhar uma sub-rede comum com a entidade identificada pelo endereço IPv6 global transportado no campo Network Address of Next Hop e o peer ao qual a rota está sendo anunciada. Em todos os outros casos, um locutor de BGP deve anunciar ao seu peer no campo Endereço de rede apenas o endereço IPv6 global do salto seguinte.

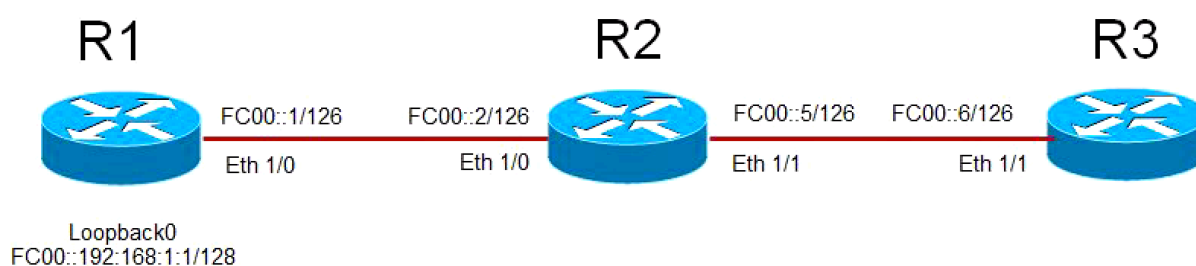
Basicamente, significa que se você tem uma relação de vizinhança IPv6 EBGP na sub-rede diretamente conectada, ele transporta o IP Link Local e o endereço IPv6 Global como um salto seguinte. No entanto, o RFC (Request for Command, Solicitação de Comando) não especifica qual deve ser preferido. A Cisco prefere o endereço de Link local porque, enquanto envia o pacote, é sempre a distância mais curta. Quando você usa o RTBH, pode ser um problema e este documento explica como lidar com ele.

Configurar

Este documento usa um caso de uso para explicar o comportamento e os comandos usados para fazer o RTBH funcionar.

Diagrama de Rede

Esta imagem é usada como uma topologia de exemplo para o restante deste documento.



- R1 tem relação de vizinhança de EBGP com R2 e R2 tem relação de vizinhança de EBGP com R3.
- O roteador R1 anuncia seu loopback 0 (FC00::192:168:1:1/128) via BGP para R2 e R2 anuncia-o para R3.
- R3 usa um mapa de rota para definir o próximo salto para o prefixo de loopback de R1 para um endereço IPv6 fictício que aponta para "NULL 0" na tabela de roteamento.

Configuração relevante

Essa configuração é usada em roteadores diferentes para simular uma situação em que o RTBH seria usado:

R1

```
interface Ethernet1/0
  no ip address
  ipv6 address FC00::1/126
end
!
interface Loopback0
  ip address 192.168.1.1 255.255.255.0
  ipv6 address FC00::192:168:1:1/128
  !
  router bgp 65500
  bgp router-id 192.168.1.1
  bgp log-neighbor-changes
  neighbor FC00::2 remote-as 65501
  !
  address-family ipv6
network FC00::/126
  network FC00::192:168:1:1/128
  neighbor FC00::2 activate
```

R2

```
interface Ethernet1/0
  no ip address
  ipv6 address FC00::2/126
end
!
interface Ethernet1/1
  no ip address
  ipv6 address FC00::5/126
  !
router bgp 65501
  bgp router-id 192.168.1.2
  bgp log-neighbor-changes
  neighbor FC00::1 remote-as 65500
  neighbor FC00::6 remote-as 65502
  !
  address-family ipv6
  network FC00::/126
  network FC00::4/126
  neighbor FC00::1 activate
  neighbor FC00::6 activate
```

R3

```
interface Ethernet1/1
  no ip address
  ipv6 address FC00::6/126
end
!
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
  match ipv6 address prefix-list BLACKHOLE-PREFIX
  set ipv6 next-hop FC00::192:168:1:3
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
  bgp router-id 192.168.1.3
  bgp log-neighbor-changes
  neighbor FC00::5 remote-as 65501
```

```
!  
address-family ipv6  
network FC00::4/126  
neighbor FC00::5 activate  
neighbor FC00::5 route-map BLACKHOLE-PBR in
```

Verificar

Caso de teste 1

Quando não houver roteamento baseado em política (PBR) configurado em R3, na tabela de roteamento, roteie para o loopback de R1 em R3 pontos para o endereço link local **FE80::A8BB:CCFF:FE00:A211**.

BGP Configuration

```
router bgp 65502  
  bgp router-id 192.168.1.3  
  bgp log-neighbor-changes  
  neighbor FC00::5 remote-as 65501  
  !  
  address-family ipv6  
  network FC00::4/126  
  neighbor FC00::5 activate
```

BGP has both next-hops.

```
R3#show bgp ipv6 unicast FC00::192:168:1:1/128  
BGP routing table entry for FC00::192:168:1:1/128, version 4  
Paths: (1 available, best #1, table default)  
  Not advertised to any peer  
  Refresh Epoch 1  
  65501 65500  
    FC00::5 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)  
      Origin IGP, localpref 100, valid, external, best  
      rx pathid: 0, tx pathid: 0x0
```

Routing Table has Link Local address as the next-hop.

```
R3#show ipv6 route FC00::192:168:1:1  
Routing entry for FC00::192:168:1:1/128  
  Known via "bgp 65502", distance 20, metric 0, type external  
  Route count is 1/1, share count 0  
  Routing paths:  
    FE80::A8BB:CCFF:FE00:A211, Ethernet1/1  
      MPLS label: nolabel  
      Last updated 00:02:45 ago
```

Destination is reachable

```
R3#ping ipv6 FC00::192:168:1:1  
Type escape sequence to abort.
```

Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Teste do caso 2

Quando há PBR configurado usando o mapa de rota **BLACKHOLE-PBR** em R3, observa-se que para **FC00::192:168:1:1/128** (loopback de R1), o próximo salto na tabela de roteamento ainda aponta para o endereço local de link **FE80: A8BB:CCFF:FE00:A211**. Portanto, o tráfego nunca é ocultado em preto e, em vez disso, roteado usando endereços locais de link.

BGP Configuration

```
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
  match ipv6 address prefix-list BLACKHOLE-PREFIX
  set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
  bgp router-id 192.168.1.3
  bgp log-neighbor-changes
  neighbor FC00::5 remote-as 65501
  !
  address-family ipv4
    no neighbor FC00::5 activate
  exit-address-family
  !
  address-family ipv6
    network FC00::4/126
    neighbor FC00::5 activate
  neighbor FC00::5 route-map BLACKHOLE-PBR in
```

Next-hop in BGP changes to the one defined in route-map.

```
R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65501 65500
    FC00::192:168:1:3 (FE80::A8BB:CCFF:FE00:A211) from FC00::5 (192.168.1.2)
      Origin IGP, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

New next-hop is not reachable and points to Null 0

```
R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    directly connected via Null0
      Last updated 00:19:23 ago
```

Routing table still uses Link Local address as next-hop.

```
R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
  Known via "bgp 65502", distance 20, metric 0, type external
  Route count is 1/1, share count 0
  Routing paths:
FE80::A8BB:CCFF:FE00:A211, Ethernet1/1
    MPLS label: nolabel
    Last updated 00:00:41 ago
```

Destination is still reachable.

```
R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Caso de teste 3

Para superar esse comportamento, use o comando de configuração de vizinho BGP **disable-connected-check** em R3. Disable-connected-check é usado para supor que o endereço IPv6 do vizinho é apenas um caminho de salto. O cenário mais comum em que esse comando é usado é quando a relação de vizinhança do EBGP é estabelecida em loopbacks para roteadores conectados diretamente. Nesse caso, o comando dá a impressão de que os roteadores estão criando uma relação de vizinhança de EBGP e não estão em uma sub-rede comum. A vizinhança pode ser entre loopbacks e, portanto, um roteador enquanto anuncia o prefixo que não carrega o endereço local do link, mas apenas o endereço IPv6 global.

Quando esse comando for adicionado, você poderá ver que a rota para o loopback de R1 **192:168:1:1/128** na tabela de roteamento de R3, aponta para o próximo salto de acordo com o mapa de rota **FC00::192:168:1:3**. Agora, como **FC00::192:168:1:3** tem uma rota apontando para Nulo 0, portanto, o tráfego está em negrito.

BGP Configuration

```
ipv6 prefix-list BLACKHOLE-PREFIX seq 5 permit FC00::192:168:1:1/128
!
route-map BLACKHOLE-PBR permit 10
  match ipv6 address prefix-list BLACKHOLE-PREFIX
  set ipv6 next-hop FC00::192:168:1:3
!
route-map BLACKHOLE-PBR permit 20
!
router bgp 65502
  bgp router-id 192.168.1.3
  bgp log-neighbor-changes
  neighbor FC00::5 remote-as 65501
  neighbor FC00::5 disable-connected-check
!
```

```
address-family ipv4
no neighbor FC00::5 activate
exit-address-family
!
address-family ipv6
network FC00::4/126
neighbor FC00::5 activate
neighbor FC00::5 route-map BLACKHOLE-PBR in
```

Next-hop in BGP changes to the one defined in route-map. There is no Link Local Address.

```
R3#show bgp ipv6 unicast FC00::192:168:1:1/128
BGP routing table entry for FC00::192:168:1:1/128, version 4
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65501 65500
FC00::192:168:1:3 from FC00::5 (192.168.1.2)
Origin IGP, localpref 100, valid, external, best
rx pathid: 0, tx pathid: 0x0
```

Routing table uses the new next-hop.

```
R3#show ipv6 route FC00::192:168:1:1
Routing entry for FC00::192:168:1:1/128
Known via "bgp 65502", distance 20, metric 0, type external
Route count is 1/1, share count 0
Routing paths:
FC00::192:168:1:3
MPLS label: nolabel
Last updated 00:00:37 ago
```

New next-hop is pointed to Null 0. Traffic will be dropped.

```
R3#show ipv6 route FC00::192:168:1:3
Routing entry for FC00::192:168:1:3/128
Known via "static", distance 1, metric 0
Route count is 1/1, share count 0
Routing paths:
directly connected via Null 0
Last updated 02:18:03 ago
```

Destination is not reachable

```
R3#ping ipv6 FC00::192:168:1:1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FC00::192:168:1:1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Note: Um novo aprimoramento [CSCuv60686](#) altera esse comportamento para que o mapa de rota entre em vigor sem usar o comando **disable-connected-check**.

Troubleshoot

No momento, não há informações de solução de problemas específicas disponíveis para este

documento.